UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

SAMSUNG ELECTRONICS CO, LTD., et al., Plaintiffs, v. BLAZE MOBILE, INC., et al., Defendants.	Case No. 21-cv-02989-EJD **ORDER GRANTING SAMSUNG'S MOTION UNDER FED. R. CIV. P. 12(C) FOR JUDGMENT OF UNPATENTABILITY UNDER 35 U.S.C. § 101 AS TO NFC SECURITY PATENTS AND DENYING MOTION AS TO MOBILE PAYMENT PATENTS** Re: ECF No. 47

Plaintiffs Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") initiated this action for a declaratory judgment of non-infringement as to eight patents (the "Patents-in-Suit") owned by Defendants Blaze Mobile, Inc. ("Blaze Mobile") and Michelle Fisher ("Fisher," and with Blaze Mobile, "Blaze"). Blaze answered and counterclaimed for infringement. Following the completion of the pleadings, Samsung moved pursuant to Federal Rule of Civil Procedure 12(c) for a judgment of unpatentability under 35 U.S.C. § 101. ECF No. 47 ("Motion" or "Mot."). Blaze filed an opposition with an appendix identifying representative claims for the Patents-in-Suit for purposes of addressing Samsung's Motion, ECF No. 50 ("Opp."), and Samsung filed a reply, ECF No. 52 ("Reply"). The Court conducted a hearing on May 12, 2022. On September 30, 2022, the Court issued an order denying Samsung's Motion as to one of three categories of Patents-in-Suit, the Advertising Patents. ECF No. 87. The Court now enters this separate Order GRANTING Samsung's Motion as to the NFC Security Patents and DENYING the Motion as to the Mobile Payment Patents.

I. BACKGROUND

A. Factual Background

Fisher is the cofounder and CEO of Blaze Mobile, and the named inventor on the following eight Patents-in-Suit, which are directed to performing a variety of functions on a mobile device:

- U.S. Patent No. 9,378,493, ("the '493 Patent") is entitled "Mobile Communication Device Near Field Communication (NFC) Transactions";
- U.S. Patent No. 9,652,771, ("the '771 Patent") is entitled "Induction Based Transactions at a Mobile Device with Authentication";
- U.S. Patent No. 9,996,849, ("the '849 Patent") is entitled "Remote Delivery of Advertisements";
- U.S. Patent No. 10,339,556, ("the '556 Patent") is entitled "Selecting and Transmitting an Advertisement from a Server in Response to User Input";
- U.S. Patent No. 10,621,612, ("the '612 Patent") is entitled "Displaying an Advertisement in Response to User Input Using a Non-Browser Based Application";
- U.S. Patent No. 10,699,259, ("the '259 Patent") is entitled "Remote Transaction Processing Using a Mobile Device";
- U.S. Patent No. 10,565,575, ("the '575 Patent") is entitled "NFC Mobile Device Transactions with a Digital Artifact"; and
- U.S. Patent No. 10,825,007, ("the '007 Patent") is entitled "Remote Transaction Processing of at a Transaction Server."

Fisher has assigned the Patents-in-Suit to Blaze Mobile. The '849, '556, and '612 are collectively referred to as the "Advertising Patents"; the '493, '771, and '575 are referred to as the "NFC Security Patents"; and the '259 and '007 are referred to as the "Mobile Payment Patents." The Court previously denied Samsung's Motion with respect to the Advertising Patents, and it does not discuss those patents here.

1. The NFC Security Patents

Blaze alleges that the NFC Security Patents "relate to security improvements in NFC enabled mobile devices, NFC point-of-sale terminals, and servers for processing an NFC payment using an identification code transmitted from a secure element embedded in the NFC enabled mobile device to the server and processing the payment at the server using the identification code." Blaze's Counterclaims for a Judgment of Patent Infringement ("Blaze Counterclaims"), ECF No. 30 ¶ 20.[1] Further, Blaze alleges that "[t]he secure transactions performed by the Accused Samsung Pay Products are a material part of the claims of the [NFC Security] Patent[s], because the Accused Samsung Pay Products perform the key inventive functions of the [NFC Security] Patent[s]." *Id.* ¶¶ 71, 108, 145.

2. The Mobile Payment Patents

Blaze alleges that the Mobile Payment Patents "relate to security improvements in non-browser mobile applications running on a mobile device, management server, and transaction server using an identification code transmitted from a non-browser-based application running on the mobile device." Blaze Counterclaims ¶ 21. Blaze further alleges that "[t]he secure transactions performed by the Accused Samsung Galaxy Store Products are a material part of the claims of the [Mobile Payment] Patent[s] because the Accused Samsung Pay Products perform the key inventive functions of the [Mobile Payment] Patent[s]." *Id.* ¶¶ 185, 224.

B. Procedural Background

Samsung filed this suit requesting a declaratory judgment of non-infringement of the eight Patents-in-Suit on April 25, 2021. ECF No. 1 ("Compl."). Blaze filed its Answer and Counterclaims alleging infringement of the Patents-in-Suit on September 13, 2021. ECF No. 30. Samsung then filed its Answer to the Blaze Counterclaims as well as its Counterclaims in Reply on September 27, 2021, and Blaze filed its Answer to Samsung's Counterclaims in Reply on October 18, 2021. ECF Nos. 38, 41.

On October 29, 2021, Samsung filed the pending Motion. ECF No. 47. Briefing was

[1] ECF No. 30 includes both Blaze's Answer and Affirmative Defenses to Samsung's Complaint for Declaratory Judgment (pp. 1–11) and the Blaze Counterclaims (pp. 11–66). The Blaze Counterclaims restart the paragraph numbering, and paragraph citations to the Blaze Counterclaims therefore refer to the second set of paragraphs in the document.

complete on November 26, 2021, and the Court heard oral argument on May 12, 2022. *See* ECF Nos. 52, 74. On September 30, 2022, the Court issued an order denying Samsung's Motion as to the Advertising Patents. ECF No. 87 (the "Prior Order").

In addition to bringing this litigation, Samsung filed requests with the United States Patent and Trademark Office's (the USPTO) Patent Trial and Appeal Board (PTAB) for *inter partes* review (IPR) of each of the Patents-in-Suit. *See* Mot. at 2. The PTAB declined to institute IPRs on the Patents-in-Suit, and denied Samsung's requests for rehearing of the denial of the Advertising Patents and the NFC Security Patents. *See* ECF No. 70 & Exhibits A–H; ECF No. 86 & Exhibits A–F (Blaze's Statements of Recent Decisions). The parties have since informed the Court that Samsung has filed requests for *ex parte* reexamination of the eight Patents-in-Suit, and that all eight requests remain pending. ECF Nos. 91, 92.

II. LEGAL STANDARDS[2]

A. Federal Rule of Civil Procedure 12(c)

A motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c) challenges the legal sufficiency of the opposing party's pleadings and operates like a motion to dismiss under Rule 12(b)(6). *Morgan v. Cnty. of Yolo*, 436 F. Supp. 2d 1152, 1154–55 (E.D. Cal. 2006). "[T]he same standard of review applicable to a Rule 12(b) motion applies to its Rule 12(c) analog," because the motions are "functionally identical." *Dworkin v. Hustler Mag., Inc.*, 867 F.2d 1188, 1192 (9th Cir. 1989). The Court will "accept factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). A district court generally may not consider materials beyond the pleadings in evaluating a Rule 12(c) motion. *Heliotrope Gen., Inc. v. Ford Motor Co.*, 189 F.3d 971, 981 n.18 (9th Cir. 1999). The court may, however, consider materials properly subject to judicial notice or incorporation by reference. *Khoja v.*

[2] As there has been no change in the relevant legal standards, this recitation of the standards is largely taken from the Prior Order.

Orexigen Therapeutics, 899 F.3d 988, 998 (9th Cir. 2018). Judgment on the pleadings is appropriate if, assuming the truth of all materials facts pled in the complaint, the moving party is entitled to judgment as a matter of law. *Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc.*, 896 F.2d 1542, 1550 (9th Cir. 1989).

B. 35 U.S.C. § 101

"Patent eligibility under § 101 is a question of law that may involve underlying questions of fact." *MyMail, Ltd. v. ooVoo, LLC*, 934 F.3d 1373, 1379 (Fed. Cir. 2019); *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1364–65 (Fed. Cir. 2018). "Not every § 101 determination contains genuine disputes over the underlying facts material to the § 101 inquiry." *Berkheimer*, 881 F.3d at 1368. A court may decide the issue of § 101 validity on a Rule 12(c) motion even if there are factual disputes, so long as it construes all allegations in favor of the non-moving party. *See SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018); *MyMail, Ltd. v. OoVoo, LLC*, 613 F. Supp. 3d 1142, 1149 (N.D. Cal. 2020) ("Accordingly, a district court may resolve the issue of patent eligibility under § 101 by way of a motion for judgment on the pleadings.") (citing *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1352 (Fed. Cir. 2014)). Where the moving party seeks a judgment of invalidity, it bears the burden demonstrating patent-ineligibility by clear and convincing evidence. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1319–20 (Fed. Cir. 2019) (citing *Microsoft Corp. v. i4i Ltd. P'ship*, 564 U.S. 91, 100 (2011)).

Section 101 of the Patent Act provides that a patent may be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. However, the Supreme Court has recognized that these broad categories contain an implicit exception: "[l]aws of nature, natural phenomena, and abstract ideas are not patentable." *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013) (internal quotation marks and citation omitted). In applying this exception, courts "must distinguish between patents that claim the building blocks of human ingenuity and those that integrate the building blocks into something more." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014) (internal quotations and citation omitted). The novelty and nonobviousness of claims under 35 U.S.C. §§ 102 and 103—*i.e.*, the available bases upon which a petitioner may request an IPR, 35 U.S.C. § 311(b)—do not bear on whether claims are directed to patent-eligible subject matter under § 101. *Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329, 1336 (Fed. Cir. 2017).

In *Alice*, the Supreme Court established a two-step framework to determine whether a claim falls within the "abstract idea" exception. First, the court must "determine whether the claims at issue are directed to a patent-ineligible concept." *Alice*, 573 U.S. at 217. This inquiry is a "meaningful one" and "cannot simply ask whether the claims involve a patent-ineligible concept, because essentially every routinely patent-eligible claim involving physical products and actions involves a law of nature and/or natural phenomenon." *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (2016). "Rather, the . . . inquiry applies a stage-one filter to claims, considered in light of the specification, based on whether 'their character as a whole is directed to excluded subject matter.'" *Id.* (citation omitted).

Second, if the claims are directed to patent-ineligible subject matter, the Court must "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 78 (2012)). The Supreme Court has described this as a search for an "inventive concept"—*i.e.*, an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Mayo*, 566 U.S. at 72–73. When assessing patent protection under § 101, the claims of the patent "must be considered as a whole." *Diamond v. Diehr*, 450 U.S. 175, 188 (1981). "This is particularly true in a process claim because a new combination of steps in a process may be patentable even though all the constituents of the combination were well known and in common use before the combination was made." *Id.*

III. DISCUSSION

Samsung contends that the NFC Security Patents and the Mobile Payment Patents should be held invalid under 35 U.S.C. §101—and the infringement claims asserting them should be dismissed—because they are directed to abstract ideas and fail to incorporate an inventive concept. Mot. at 1. In response, Blaze asserts that Samsung's Motion should be denied because the NFC Security Patents and the Mobile Payment Patents involve disputed claim terms that must be construed, the Motion raises genuine disputes of material fact, which are not suitable for resolution on the pleadings, and each of the Patents-in-Suit is directed to a technical solution to a technical problem—not an abstract idea—and recites an inventive concept. Opp. at 9–10, 16.

A. Claim Construction

The Court rejects Blaze's assertion that a § 101 invalidity analysis is premature in this case without first conducting claim construction. As explained in the Prior Order, ECF No. 87 at 5–6, Blaze "has not explained how it might benefit from any particular term's construction under an *Alice* § 101 analysis." *Simio, LLC v. FlexSim Software Prods., Inc.*, 983 F.3d 1353, 1365 (Fed. Cir. 2020). Rather, Blaze identifies disputed terms "non-browser based application," "secure element," and "secure element application" and then relies on the Federal Circuit's general guidance that claim construction is desirable, and often necessary prior to a § 101 analysis, for "a full understanding of the basic character of the claimed subject matter." *StoneEagle Servs., Inc. v. Pay-Plus Sols., Inc.*, 2015 WL 518852 * 4 (M.D. Fla. 2015) (quoting *Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can. (U.S.)*, 687 F.3d 1266, 1273–74 (Fed. Cir. 2012)). "[M]erely point[ing] to the claim language," without explaining how claim construction would change the analysis is insufficient to defer consideration of the instant motion. *See Cyberfone Sys., LLC v. CNN Interactive Grp., Inc.*, 558 F. App'x. 988, 991 n.1 (Fed. Cir. 2014) (patentee made insufficient showing that claim construction was necessary to resolve § 101 challenge in light of failure to "explain which terms require construction or how the [§ 101] analysis would change").

B. Factual Disputes

The Court also again rejects Blaze's blanket assertion that Samsung's motion is premature because of factual disputes. *See* Prior Order at 6. "[C]ourts can, and regularly do, decide the issue of § 101 invalidity on a Rule 12(c) motion." *Barbaro Techs., LLC v. Niantic, Inc.*, 475 F. Supp. 3d 1007, 1011 (N.D. Cal. 2020); *see also SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018) (noting § 101 invalidity "may be, and frequently has been, resolved on a Rule 12(b)(6) or (c) motion"). When the issue of § 101 invalidity is raised at the pleading stage "it simply means all allegations must be accepted as true and construed in the light most favorable to the non-moving party." *Barbaro*, 475 F. Supp. 3d at 1011; *see also Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018) (patent eligibility can be determined at the Rule 12(b)(6) stage "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law.").

C. Patent Eligibility Under 35 U.S.C. § 101

The Court evaluates the patent eligibility of the NFC Security Patents and the Mobile Payment Patents under the *Alice* test. *See Alice*, 573 U.S. at 217–18.

1. The NFC Security Patents

The NFC Security Patents are directed to securely processing near field communication (NFC) transactions made by mobile devices. *See, e.g.*, ECF No. 1-1 ("'493 Patent"), claim 9.[3] Claim 9 of the '493 Patent recites:

> **9.** A mobile device using a near field communication protocol for an NFC transaction, the mobile communication device comprising:
>
> a mobile device memory;
>
> a mobile device processor; and
>
> a mobile device transceiver;

[3] Blaze submits claim 9 of the '493 Patent as a representative claim for the NFC Security Patents. Opp., App'x A at 1. After reviewing the NFC Security Patents' claims, the Court is satisfied that claim 9 of the '493 Patent is representative of the remaining claims. The Court will nonetheless also recite a method claim as a further example of the claims at issue.

> wherein the mobile device is associated with a secure element, the secure element including a secure element memory, a secure element-processor, a secure element communication transceiver supporting a first communication channel comprising the near field communications (NFC) protocol, wherein the secure element memory maintains a secure element application config used to use the NFC protocol and an identification code, wherein the secure element application is executed by the secure element processor in response to detection of a near field communication inductive signal by an NFC terminal and execution of the secure element application facilitates transfer of the identification code to the NFC terminal the secure element communication transceiver and further wherein the NFC terminal transfers the identification code to a management server which transmits the identification code to a transaction server for processing of the NFC transaction using a payment method corresponding to the identification code, the NFC terminal configured to use the NFC protocol.

Id. Claim 1 of the ’493 Patent—the only other independent claim—recites a related method:

> **1.** A method for conducting a Near Field Communications (NFC) transaction using an N[F]C protocol and a mobile communication device, the method comprising:
>
> maintaining a secure element application configured to use the NFC protocol and an identification code in a secure element memory in a secure element, the secure element, associated with a mobile communication device comprising of a mobile device memory, a mobile device processor, and a mobile device transceiver, the secure element including the secure element memory, a secure element processor and a secure element communication transceiver supporting a communication channel comprising the (NFC) protocol;
>
> executing the secure element application, wherein the secure element application is executed by the secure element processor in response to detection of a near field communication inductive signal by an NFC terminal, and execution of the secure element application facilitates transfer of the identification code to the NFC terminal using the NFC protocol, and further wherein the NFC terminal transfers the identification code to a management server which transmits the identification code to a transaction server for processing of the NFC transaction using a payment method corresponding to the identification code, wherein the NFC terminal is configured to use the NFC protocol.

Id. Further, independent claim 19 of the ’771 Patent recites a claim for computer code for a mobile application capable of implementing the above-described NFC processes. *See* ECF No. 1-

2 ("'771 Patent"), claim 19.[4]

a. *Alice* Step One: Whether the NFC Security Patents are Directed to an Abstract Idea

Samsung contends that the NFC Security Patents are directed to the abstract concept of providing security for transactions on mobile devices. Mot. at 11–15. Blaze asserts that the NFC Security Patents instead relate to "security improvements in NFC-enabled mobile devices, NFC point-of-sale terminals, and servers for processing NFC payments using an identification code transmitted from a secure element in the NFC-enabled mobile device to the server." Opp. at 10. As described in the representative claim, the security process of the claimed invention is essentially as follows: (1) the mobile device's "secure element" detects an NFC signal (*e.g.*, a cellphone is placed close to a tap-to-pay point-of-sale terminal at a merchant's location); (2) upon this detection, the secure element activates a related "secure element application"; (3) the app transfers the secure element's identification code to the point-of-sale device; (4) the point-of-sale device transfers that identification code to a management server; (5) the management server in turn transmits the identification code to a transaction server; and (6) the transaction server processes the transaction using payment information corresponding to the identification code. '493 Patent, claim 9.

Whether or not an idea is abstract is generally determined by "compar[ing] claims at issue to those claims already found to be directed to an abstract idea in previous cases." *Enfish*, 822 F.3d at 1334. "[F]undamental economic and conventional business practices are often found to be abstract ideas, even if performed on a computer." *Id.* at 1335 (citation omitted). Courts have repeatedly found that increasing the security of a payment transaction is an abstract concept directed to a fundamental economic practice. *See, e.g.*, *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1353 (Fed. Cir. 2021) ("Moreover, as we have previously explained, verifying

[4] The Patents-in-Suit in suit are all attached as exhibits to Samsung's Complaint and necessarily form the basis for this action. As such, they are incorporated by reference and the Court may (and indeed, must) consider them. *See Khoja v. Orexigen*, 899 F.3d 988, 998 (9th Cir. 2018).

the identity of a user to facilitate a transaction is a fundamental economic practice that has been performed at the point of sale well before the use of POS computers and Internet transactions.") (citation omitted); *Innovation Scis., LLC v. Amazon.com, Inc.*, 778 F. App'x 859, 863 (Fed. Cir. 2019) ("We agree with the district court that claim 17 is directed to the abstract idea of securely processing a credit card transaction with a payment server.").

The purpose of securing a transaction is to ensure that the exchange of sensitive (generally financial) information required for a purchase does not result in that information falling into the hands of a wrongdoer who might use it to perpetrate fraudulent activity, or to prevent such a wrongdoer from using the ill-gotten information to make a purchase. The NFC Security Patents appear to be squarely aimed at the abstract, fundamental economic practice of facilitating secure transactions—here, by authenticating the proper payment method for NFC transactions via an identification code received through a series of transfers beginning with a secure application on a mobile device. The impetus for the invention was the public's increasing use of mobile devices to conduct payment transactions and the resulting "critical [need] to protect a user from fraudulent usage due to, e.g., loss or theft of a mobile communication device." '493 Patent, Background of the Invention. And even outside of the payment context, "controlling access to data" for security purposes is an abstract concept. *Dropbox, Inc. v. Synchronoss Techs., Inc.*, 815 F. App'x 529, 532 (Fed. Cir. 2020); *see also Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) ("Under step one, the . . . asserted claims are directed to the abstract idea of 'providing restricted access to resources.'").

"In cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself." *Universal Secure Registry*, 10 F.4th at 1346. Blaze argues the NFC Security Patents provide a technical solution for the "problem of storing sensitive personal information (such as credit card information) on a mobile device that can be lost or stolen" through the claimed ordered combination of the patent limitations. Opp. at 11. Blaze also contrasts the NFC Security Patents, which it claims "improve security and scalability by providing a secure element and a secure element application," with the claims at issue in *Innovation Sciences* that the court found did not "purport to improve the payment server or the [listing] server." *Id.* at 13 (citation omitted).

These arguments are not persuasive, as the NFC Security Patents' claims do not provide sufficient specificity to constitute an improvement in functionality. The representative claim of the '493 Patent first recites an NFC-enabled mobile device with a memory, processor, and transceiver. '493 Patent, claim 9. There is no suggestion that well-known NFC technology added to the basic building blocks of a computer is an improvement. *See Alice*, 573 U.S. at 217. The rest of the claim provides that the mobile device is "associated" with a secure element (itself including a memory, processor, and transceiver) that "maintains" an NFC-enabled application that is "executed" upon "detection" of an NFC signal, following which an identification code held in the secure element is "transfer[red]" or "transmit[ted]" to servers until the payment is "processed." '493 Patent, claim 9. This process is exceedingly similar to that described in *Universal Secure Registry*:

> (1) "receiving" a transaction request with a time-varying multicharacter code and "an indication of" the merchant requesting the transaction; (2) "mapping" the time-varying multicharacter code to the identity of the customer in question; (3) "determining" whether the merchant's access to the customer's secure data complies with any restrictions; (4) "accessing" the customer's account information; (5) "providing" the account identifying information to a third party without providing that information to the merchant; and (6) "enabling or denying" the merchant to perform the transaction without obtaining knowledge of the customer's identifying information.

10 F.4th at 1349 (citation omitted). Consistent with *Universal Secure Registry*, this Court finds that the NFC Security Patents are directed to the abstract idea of "a method for enabling a transaction between a user and a merchant" that uses a "code instead of the user's secure (credit card) information." *Id.*

The Court therefore finds that the claims in the NFC Security Patents "simply recite conventional actions in a generic way"—here, a phone that "maintains" and "executes" an application that "transfers" a code that allows a more secure transaction—and are directed to an abstract idea. *See id.* Further, the NFC Security Patents describe the effects of the required tasks for the security process (maintaining, detecting, executing, transferring), but do not "explain[] how to accomplish any of the tasks." *Int'l Bus. Machs. Corp. v. Zillow Grp., Inc.*, 50 F.4th 1371, 1378 (Fed. Cir. 2022). Such claims that "'merely describe an effect or result dissociated from any method by which [it] is accomplished' [are] usually 'not directed to patent-eligible subject matter.'" *Id.* (quoting *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1244 (Fed. Cir. 2016)). The Court concludes that the NFC Security Patents are directed to an ineligible abstract idea.

b. *Alice* Step Two: Whether the NFC Security Patents Add an Inventive Concept to the Abstract Idea

Because the NFC Security Patents are directed to an abstract idea, the Court turns to the second step of *Alice* and "consider[s] the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo*, 566 U.S. at 78). An inventive concept in the claims "must be more than well-understood, routine, conventional activity," "and cannot simply be an instruction to implement or apply the abstract idea on a computer." *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016). That is, the inventive concept "must be significantly more than the abstract idea itself." *Universal Secure Registry*, 10 F.4th at 1350.

Prism Technologies is instructive here. The Federal Circuit held that the district court erred in its conclusion that the asserted claims included inventive concepts because they "modif[ied] the way the Internet functions to provide secure access over a protected computer resource." 696 F. App'x at 1017. The claims at issue "merely recited a host of elements"—including an "authentication server," "access server," "Internet Protocol network," and "client computer device"—that were "indisputably generic computer components." *Id.* Prism argued that the claims' combination of these generic components with certain recited "identity data" yielded a "novel, effective solution to real-world problems." *Id.* at 1018. The circuit court held that identity data, such as hardware identifiers, were in fact conventional, and that there was "no indication that their inclusion produce[d] ‘a result that over[rode] the routine and conventional’ use of this known feature.” *Id.* Because the asserted claims, even when viewed as an ordered combination, “recite[d] no more than the sort of ‘perfectly conventional’ generic computer components employed in a customary manner,” the claims failed step two of *Alice*.

The NFC Security Patents include a similar “host of elements” that are generic computer components, such as a “management server,” “transaction server,” “NFC protocol,” and “mobile [communication] device” with a memory, processor, and transceiver. *See, e.g.*, ’493 Patent, claim 9. And just as Prism pointed to “identity data,” Blaze argues that the NFC Security Patents’ “use of a ‘secure element’ and ‘secure element application,’ in the ordered combination . . . constitutes an inventive concept because it improves the security, performance, and scalability of an NFC-enabled mobile device.” Opp. at 15. Blaze does not argue that the secure element and secure element application components of the NFC Security Patents are themselves Blaze’s inventive concepts, outside of the claimed ordered combination. *See id.* at 16. In fact, as in *Prism*, the “patents[] themselves demonstrate the conventional nature” of both of these items. 696 F. App’x at 1018. Fisher’s patent application no. 11/467,441[5] explains that an illustration showed “the secure element [] associated with the mobile device [], *the secure element [] being commonly known as a smart card*. As illustrated, the secure element [] has a secure processor [], a secure memory [], and a . . . transceiver [].” ECF No. 51-2 (“’441 Patent”) ¶ 33 (emphasis added). The ’441 Patent also explained that “*various software* that is downloaded that is downloaded into . . . the secure memory . . . of the secure element . . . [and] *implemented using based upon [sic] known knowledge* of mobile device . . . internals and application platforms, NFC, smartcard internals and application platforms, payment protocols . . . transaction, and management servers.” *Id.* ¶ 40 (emphases added). In prosecuting the ’493 Patent, the applicants relied on this and similar statements to argue that the “secure element application” recited in the ’493 Patent was

[5] The NFC Security Patents all incorporate by reference Patent Application No. 11/467,441. *See, e.g.*, ’493 Patent, col. 1:34–39.

contemplated by the ’441 Patent, so that the ’493 Patent was not invalidated by prior art introduced in the period between the applications of the ’441 Patent and the ’493 Patent. ECF No. 47-2 (“’493 History Excerpts”) at 4. The secure element and secure element application are therefore also conventional computer components.[6]

The only question, then, is whether the claimed ordered combination is an inventive concept. Unfortunately for Blaze, there is no indication in the NFC Security Patents, the pleadings, or Blaze’s written or oral submissions that the inclusion of the secure element or secure element application “produces ‘a result that overrides the routine and conventional’ use of th[ese] known feature[s].” *Prism*, 696 F. App’x at 1018. Blaze argues that both (1) “the use of a secure element and secure element application that stores an identification code separately from the main mobile device memory” and (2) “storing the credit card information (i.e., ‘payment method’) at the remote management server” were “departure[s] from conventional approaches.” Opp. at 15. But the provision of an identification code from a secure source apart from a mobile device is not an inventive concept. *Universal Secure Registry*, 10 F.4th at 1353 (finding authentication code “generated by the ‘SecurIDTM card available from RSA Security,’ as well as ‘other smart cards,’” to be a “conventional authentication technique[]”). Nor is the “stor[age] [of] account information, such as credit card and debit card account information,” in a secure location apart from a “user device (e.g., cell phone)” an inventive concept. *See id.* at 1351.

The Prior Order found that Blaze had recited a plausible inventive concept as to the Advertising Patents because those patents permitted advertising content to be displayed on a non-browser based application without connection to a server. Prior Order at 14–15. Although one of the NFC Security Patents—the ’575 Patent—includes dependent claims reciting a non-browser based application that is operative when the mobile device is not connected to a wireless network,

[6] Consistent with this principle, Blaze alleges that “Samsung’s Secu-NFC Chip [] enables secure mobile payments by combining an NFC controller and a secure element storing personal information . . . [and] contains . . . a secure element application,” but its infringement allegations are based on the claimed ordered combination, rather than the mere existence of Samsung’s Secu-NFC Chip. Blaze’s Counterclaims ¶¶ 34–35; *see, e.g.*, *id.* ¶¶ 31, 38, 48.

the Court does not find that Blaze has plausibly alleged the same inventive concept with respect to the NFC Security Patents. First, although this concept was central to Blaze's overview of the Advertising Patents, Blaze did not even mention a non-browser based application—let alone wireless connectivity—in its summary description of the NFC Security Patents. *Compare* Blaze Counterclaims ¶ 22 ("The [Advertising Patents] relate to improvements in the reliability and performance of non-browser mobile application running on a mobile device for delivering advertisements, for example, a coupon (*i.e.*, advertisement) which can be displayed in the non-browser based application if the mobile device is offline and loses connection with a wireless network."), *with id.* ¶ 20 ("The [NFC Security Patents] relate to security improvements in NFC enabled mobile devices, NFC point-of-sale terminals, and servers for processing an NFC payment using an identification code transmitted from a secure element embedded in the NFC enabled mobile device to the server and processing the payment at the server using the identification code."). Second, and in the same vein, Blaze did not choose as representative an NFC Security Patent that recited a non-browser based application, in contrast to its choices as to the Advertising Patents and the Mobile Payment Patents. *See* Opp., App'x A. Third, the '493 Patent and '771 Patent have no claims, independent or dependent, that mention network connectivity. Fourth, although Blaze discusses the non-browser based application and wireless connectivity with respect to the '575 Patent, these allegations relate to the construction of the term "non-browser based application." *See* Blaze Counterclaims ¶¶ 42–49. There is no other mention of wireless connectivity in Blaze's pleadings with respect to the NFC Security Patents, in contrast to the allegations regarding the Advertising Patents, where wireless connectivity is alleged in some detail with respect to all three patents. *See, e.g.*, *id.* ¶¶ 235 ('612 Patent), 267–68 ('556 Patent), 300–01 ('849 Patent). Given these differences between Blaze's allegations regarding the NFC Security Patents and the Advertising Patents, the Court finds that Blaze has not recited an inventive concept with respect to network connectivity for the NFC Security Patents.[7]

[7] Nor did Blaze argue such an inventive concept in its opposition, further demonstrating the

As described above, "[t]here is nothing in the specification suggesting, or any other factual basis for a plausible inference . . . that the claimed combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique." *Universal Secure Registry*, 10 F.4th at 1353. The Court therefore concludes, based on the clear and convincing evidence of the contents of the NFC Security Patents, that these patents fail to recite an inventive concept under *Alice* step two. The claims are thus patent-ineligible under § 101.

2. The Mobile Payment Patents

The Mobile Payment Patents are directed to securely processing product purchase transactions made by mobile devices. *See, e.g.*, ECF No. 1-6 ("'259 Patent"), claim 7.[8] Claim 7 of the '259 Patent recites:

> **7.** A mobile device for processing a transaction, comprising:
>
> a mobile device memory included in a mobile device, the mobile device memory configured to store a non-browser based application, wherein the non-browser based application is a mobile operating system platform based mobile application with a graphical user interface which includes a graphical icon that is preinstalled or downloaded and installed on the mobile device wherein the non-browser based application only generates a non-browser based application generated screen, the non-browser based application generated screen corresponding to a specific screen or area of the non-browser based application, the mobile device comprising the mobile device memory, a mobile device display;
>
> a mobile device wireless radio interface consisting of at least of a wireless fidelity (WiFi) interface and a mobile device wireless radio interface that supports voice and data interaction through a first wireless communication channel device using a lest one of GSM and CDEMA configured to:
>
> receive, at the non-browser based application generated screen, a list of products from a remote management server for display using the non-browser based application;

differences between the two groups of patents. *Compare* Opp. at 15–16 (NFC Security Patents), *with id.* at 23–25 (Advertising Patents).

[8] Blaze submits claim 7 of the '259 Patent as a representative claim for the Mobile Payment Patents. Opp., App'x A at 1–2. After reviewing the Mobile Payment Patents' claims, the Court is satisfied that claim 7 of the '259 Patent is representative of the remaining claims.

> send, from the non-browser based application generated screen, the identification of one or more products to the remote management server;
>
> send, from the non-browser base application generated screen, the transaction purchase request to the remote management server;
>
> send, from the non-browser base application generated screen, the user input login information t the remote management server;
>
> receive information authenticating the user association with the user input login information from the remote management server and further wherein the remote management server and receives transaction verification from a transaction server which processed the transaction using a payment method that corresponds to the identification code associated with the user, wherein the payment method is stored at the remote management server; wherein the transaction verification indicated that the transaction has processed; and
>
> receive, at the mobile device, the one or more products from the remote management server;
>
> a mobile device input interface configured to:
>
> receive, at the non-browser based application generated screen, an identification of one or more products selected from the list of products from non-browser based application generated screen, wherein the non-browser based application receives the identification of the one or more products selected from the list of products through user input via the mobile device display;
>
> receive a transaction purchase request from the non-browser based application generated screen, wherein the non-browser based application generated screen receives the transaction purchase request received from the user via the mobile device display and further wherein the transaction purchase request includes information relating to the identification of the one or more products; and
>
> receive user input login information including an identification code associated with the user from the non-browser based application generated screen, wherein the non-browser based application receives the user input login information through user input via the mobile device display.

Id. Of the other independent claims in the '259 Patent, claim 1 recites a method and claim 13 recites "[a] non-transitory computer readable medium," *i.e.*, computer code. *Id.* at claims 1, 13.

a. *Alice* Step One: Whether the Mobile Payment Patents are Directed to an Abstract Idea

Samsung contends that the Mobile Payment Patents are directed to the abstract idea of conducting online payment transactions on mobile devices. Mot. at 17. Blaze argues that Samsung's characterization of the claimed invention is an overly broad abstraction and does not consider the specifics of the claims. Opp. at 16.

As noted above, "fundamental economic and conventional business practices are often found to be abstract ideas." *Enfish*, 822 F.3d at 1335 (citation omitted). The Court finds that the core invention of the Mobile Payment Patents is directed to a combination of two fundamental economic practices, namely, (1) selecting and purchasing products and (2) providing security for transactions on mobile devices. As to the first practice, the representative claim recites a process by which the claimed invention "receive[s] . . . a list of products"; "send[s] . . . the identification of one or more products to the . . . server"; "send[s] . . . the transaction purchase request to the . . . server"; "processes the transaction using a payment method"; and "receive[s] . . . the one or more products." '259 Patent, claim 7. These steps are a mobile version of going to a grocery store with a shopping list, choosing the available items from the shelves, arriving at the checkout counter, paying for the products, and leaving the store with the products, and are evidently directed to an abstract idea. "No entity is entitled to 'wholly preempt' such concepts." *Inventor Holdings, LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372, 1378 (Fed. Cir. 2017) (finding "idea that a customer may pay for items ordered from a remote seller at a third-party's local establishment" to be "the type of fundamental business practice that, when implemented using generic computer technology, is not patent-eligible").

The second practice embodied in the Mobile Payment Patents is providing security for transactions on mobile devices. The patents outline a process by which the invention, following the identification of the products intended for purchase, "send[s], from the non-browser based application generated screen, the user input login information to the remote management server"; "receive[s] information authenticating the user associated with the user input login information from the remote management server"; "processes the transaction using a payment method that corresponds to the identification code associated with the user, wherein the payment method is stored at the remote management server." '259 Patent, claim 7. These steps are evidently designed to authenticate the user and enhance the security of the payment information. *See id.* at col. 3:2–9 ("One potential benefit of having payment authorizations flow through the mobile communication device [] is that sensitive user information (e.g. account numbers, pin numbers, and/or identity information) need only be sent from the mobile communication device [] directly to an issuer authorization. Such operation reduces the potential for identity theft and/or fraudulent purchases made through a point of sale device."). For the same reasons described above with respect to the NFC Security Patents, the Court finds that providing security for transactions on mobile devices is an abstract idea. *See supra*, Section III.C.1.a.

b. ***Alice* Step Two: Whether the Mobile Payment Patents Add an Inventive Concept to the Abstract Ideas**

The Court now considers whether the Mobile Payment Patents recite an inventive concept under *Alice* step two. The Mobile Payment Patents invoke generic computing components ("cellular phone," "laptop computer," "remote management server," and "non-browser based application") and activities ("send[ing]," "receiv[ing]," "display[ing]," process[ing]"). *See* '259 Patent, claim 7. Blaze nonetheless contends that the ordered combination of the inventions in the Mobile Payment Patents recite an inventive concept by presenting specific technical solutions to technical problems. Opp. at 18–20.

The Court agrees. Claims are patent-eligible even if their individual elements are generic or conventional when the ordered combination of elements provides a technical improvement over the prior art. *See Bascom*, 827 F.3d at 1350. Blaze alleges that the Mobile Payment Patents are an improvement over the prior art because, for example, "in offline mode the non-browser-based application is open and while open continues to display the digital artifact even if the mobile device loses connection with the wireless network." Blaze Counterclaims ¶ 162. This allegation is supported by the specification and claims of the Mobile Payment Patents, which provide that "consumers have the ability to store their shopping list . . . and add, delete, or change items . . . either in offline or online mode" and "the non-browser based application generated screen is operative even if the mobile device is not connected to a network." '259 Patent, col. 5:13–16; *id.*, claim 27. Samsung counters that this concept is nothing other than caching, another conventional computing function. Reply at 15. But, as noted in the Prior Order with respect to the Advertising Patents, Blaze has provided "plausible and specific factual allegations that aspects of the claims are inventive" that are sufficient to defeat a motion for judgment on the pleadings. *See* Prior Order at 15 (quoting *Cellspin*, 927 F.3d at 1317).

Accordingly, the Court finds that Blaze has plausibly alleged an inventive concept in the Mobile Payment Patents under *Alice* step two.

IV. CONCLUSION

For the reasons stated above, Samsung's Motion for a judgment of unpatentability under 35 U.S.C. § 101 is GRANTED as to the NFC Security Patents and DENIED as to the Mobile Payment Patents.

IT IS SO ORDERED.

Dated: May 16, 2023

EDWARD J. DAVILA
United States District Judge